Classified National Security Information: E.O. 12958 And Its Implementing Directives

Information Security Oversight Office

Title 3

EXECUTIVE ORDER 12958

---

60 Fed. Reg. 19825

April 17, 1995

Table of Contents

PREAMBLE

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national interest has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our participation within the community of nations. Protecting information critical to our Nation's security remains a priority. In recent years, however, dramatic changes have altered, although not eliminated, the national security threats that we confront. These changes provide a greater opportunity to emphasize our commitment to open Government.

NOW, therefore, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Part 1 - Original Classification

Sec. 1.1 *Definitions.* For purposes of this order:

(a) "National security" means the national defense or foreign relations of the United States.

(b) "Information" means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

(c) "Classified national security information" (hereafter "classified information") means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

(d) "Foreign Government Information" means:

(1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

(2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or

(3) information received and treated as "Foreign Government Information" under the terms of a predecessor order.

(e) "Classification" means the act or process by which information is determined to be classified information.

(f) "Original classification" means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

(g) "Original classification authority" means an individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance.

(h) "Unauthorized disclosure" means a communication or physical transfer of classified information to an unauthorized recipient.

(i) "Agency" means any "Executive agency," as defined in 5 U.S.C. 105, and any other entity within the executive branch that comes into the possession of classified information.

(j) "Senior agency official" means the official designated by the agency head under section 5.6(c) of this order to direct and administer the agency's program under which information is classified, safeguarded and declassified.

(k) "Confidential source" means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

(l) "Damage to the national security" means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information.

Sec. 1.2 *Classification Standards.*

(a) Information may be originally classified under the terms of this order only if all of the following conditions are met:

(1) an original classification authority is classifying the information;

(2) the information is owned by, produced by or for, or is under the control of the United States Government;

(3) the information falls within one or more of the categories of information listed in section 1.5 of this order; and

(4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security and the original classification authority is able to identify or describe the damage.

(b) If there is significant doubt about the need to classify information, it shall not be classified. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

(c) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

Sec. 1.3 *Classification Levels.*

(a) Information may be classified at one of the following three levels:

(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

(c) If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

Sec. 1.4 *Classification Authority.*

(a) The authority to classify information originally may be exercised only by:

(1) The President;

(2) agency heads and officials designated by the President in the *Federal Register* or

(3) United States Government officials delegated this authority pursuant to paragraph (c), below.

(b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

(c) Delegation of original classification authority.

(1) Delegations of original classification authority shall be limited to the minimum required to administer this order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) "Top Secret" original classification authority may be delegated only by the President or by an agency head or official designated pursuant to paragraph (a)(2), above.

(3) "Secret" or "Confidential" original classification authority may be delegated only by the President; an agency head or official designated pursuant to paragraph (a)(2), above; or the senior agency official, provided that official has been delegated "Top Secret" original classification authority by the agency head.

(4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this order. Each delegation shall identify the official by name or position title.

(d) Original classification authorities must receive training in original classification as provided in this order and its implementing directives.

(e) *Exceptional Cases.* When an employee, contractor, licensee, certificate holder, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this order and its implementing directives. The information shall be transmitted promptly as provided under this order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within 30 days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

Sec. 1.5 *Classification Categories.*

Information may not be considered for classification unless it concerns:

(a) military plans, weapons systems, or operations;

(b) foreign government information;

(c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;

(d) foreign relations or foreign activities of the United States, including confidential sources;

(e) scientific, technological, or economic matters relating to the national security;

(f) United States Government programs for safeguarding nuclear materials or facilities; or

(g) vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

Sec. 1.6 *Duration of Classification.*

(a) At the time of original classification, the original classification authority shall attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information. The date or event shall not exceed the time frame in paragraph (b), below.

(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, except as provided in paragraph (d), below.

(c) An original classification authority may extend the duration of classification or reclassify specific information for successive periods not to exceed 10 years at a time if such action is consistent with the standards and procedures established under this order. This provision does not apply to information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code.

(d) At the time of original classification, the original classification authority may exempt from declassification within 10 years specific information, the unauthorized disclosure of which

could reasonably be expected to cause damage to the national security, for a period greater than that provided in paragraph (b), above, and the release of which could reasonably be expected to:

(1) reveal an intelligence source, method, or activity, or a cryptologic system or activity;

(2) reveal information that would assist in the development or use of weapons of mass destruction;

(3) reveal information that would impair the development or use of technology within a United States weapon system;

(4) reveal United States military plans, or national security emergency preparedness plans;

(5) reveal foreign government information;

(6) damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than that provided in paragraph (b), above;

(7) impair the ability of responsible United States Government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized; or

(8) violate a statute, treaty, or international agreement.

(e) Information marked for an indefinite duration of classification under predecessor orders, for example, "Originating Agency's Determination Required," or information classified under predecessor orders that contains no declassification instructions shall be declassified in accordance with part 3 of this order.

Sec. 1.7 *Identification and Markings.*

(a) At the time of original classification, the following shall appear on the face of each classified document, or shall be applied to other classified media in an appropriate manner:

(1) one of the three classification levels defined in section 1.3 of this order;

(2) the identity, by name or personal identifier and position, of the original classification authority;

(3) the agency and office of origin, if not otherwise evident;

(4) declassification instructions, which shall indicate one of the following:

(A) The date or event for declassification, as prescribed in section 1.6(a) or section 1.6(c); or

(B) the date that is ten years from the date of original classification, as prescribed in section 1.6(b); or

(C) the exemption category from automatic declassification, as prescribed in section 1.6(d); and

(5) a concise reason for classification which, at a minimum, cites the applicable classification categories in section 1.5 of this order.

(b) Specific information contained in paragraph (a), above, may be excluded if it would reveal additional classified information.

(c) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, which portions are exempt from declassification under section 1.6(d) of this order, and which portions are unclassified. In accordance with standards prescribed in directives issued under this order, the Director of the Information Security Oversight Office may grant waivers of this requirement for specified classes of documents or information. The Director shall revoke any waiver upon a finding of abuse.

(d) Markings implementing the provisions of this order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives issued pursuant to this order.

(e) Foreign government information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information.

(f) Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Whenever such information is used in the derivative classification process or is reviewed for possible declassification, holders of such information shall coordinate with an appropriate classification authority for the application of omitted markings.

(g) The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document.

Sec. 1.8 *Classification Prohibitions and Limitations.*

(a) In no case shall information be classified in order to:

(1) conceal violations of law, inefficiency, or administrative error;

(2) prevent embarrassment to a person, organization, or agency;

(3) restrain competition; or

(4) prevent or delay the release of information that does not require protection in the interest of national security.

(b) Basic scientific research information not clearly related to the national security may not be classified.

(c) Information may not be reclassified after it has been declassified and released to the public under proper authority.

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.6 of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.6 of this order. This provision does not apply to

classified information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code.

(e) Compilations of items of information which are individually unclassified may be classified if the compiled information reveals an additional association or relationship that:

(1) meets the standards for classification under this order; and

(2) is not otherwise revealed in the individual items of information. As used in this order, "compilation" means an aggregation of pre-existing unclassified items of information.

Sec. 1.9 *Classification Challenges.*

(a) Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under paragraph (b), below.

(b) In accordance with implementing directives issued pursuant to this order, an agency head or senior agency official shall establish procedures under which authorized holders of information are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall assure that:

(1) individuals are not subject to retribution for bringing such actions;

(2) an opportunity is provided for review by an impartial official or panel; and

(3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel established by section 5.4 of this order.

Part 2 - Derivative Classification

Sec. 2.1 *Definitions.* For purposes of this order:

(a) "Derivative classification" means the incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(b) "Classification guidance" means any instruction or source that prescribes the classification of specific information.

(c) "Classification guide" means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

(d) "Source document" means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(e) "Multiple sources" means two or more source documents, classification guides or a combination of both.

Sec. 2.2 *Use of Derivative Classification.*

(a) Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) observe and respect original classification decisions; and

(2) carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:

(A) the date or event for declassification that corresponds to the longest period of classification among the sources; and

(B) a listing of these sources on or attached to the official file or record copy.

Sec. 2.3 *Classification Guides.*

(a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this order.

(b) Each guide shall be approved personally and in writing by an official who:

(1) has program or supervisory responsibility over the information or is the senior agency official; and

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agencies shall establish procedures to assure that classification guides are reviewed and updated as provided in directives issued under this order.

Part 3 - Declassification and Downgrading

Sec. 3.1 *Definitions.* For purposes of this order:

(a) "Declassification" means the authorized change in the status of information from classified information to unclassified information.

(b) "Automatic declassification" means the declassification of information based solely upon:

(1) The occurrence of a specific date or event as determined by the original classification authority; or

(2) the expiration of a maximum time frame for duration of classification established under this order.

(c) "Declassification authority" means:

(1) the official who authorized the original classification, if that official is still serving in the same position;

(2) the originator's current successor in function;

(3) a supervisory official of either; or

(4) officials delegated declassification authority in writing by the agency head or the senior agency official.

(d) "Mandatory declassification review" means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.6 of this order.

(e) "Systematic declassification review" means the review for declassification of classified information contained in records that have been determined by the Archivist of the United States ("Archivist") to have permanent historical value in accordance with chapter 33 of title 44, United States Code.

(f) "Declassification guide" means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

(g) "Downgrading" means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

(h) "File series" means documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same function or activity.

Sec. 3.2 *Authority for Declassification.*

(a) Information shall be declassified as soon as it no longer meets the standards for classification under this order.

(b) It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or the senior agency official. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

(c) If the Director of the Information Security Oversight Office determines that information is classified in violation of this order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the President through the Assistant to the President for National Security Affairs. The information shall remain classified pending a prompt decision on the appeal.

(d) The provisions of this section shall also apply to agencies that, under the terms of this order, do not have original classification authority, but had such authority under predecessor orders.

Sec. 3.3 *Transferred Information.*

(a) In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this order.

(b) In the case of classified information that is not officially transferred as described in paragraph (a), above, but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of this order. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the information.

(c) Classified information accessioned into the National Archives and Records Administration ("National Archives") as of the effective date of this order shall be declassified or downgraded by the Archivist in accordance with this order, the directives issued pursuant to this order, agency declassification guides, and any existing procedural agreement between the Archivist and the relevant agency head.

(d) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that records containing classified information be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to information being transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that goes out of existence.

(e) To the extent practicable, agencies shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification in sections 1.6 and 3.4 of this order.

Sec. 3.4 *Automatic Declassification.*

(a) Subject to paragraph (b), below, within five years from the date of this order, all classified information contained in records that (1) are more than 25 years old, and (2) have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. Subsequently, all classified information in such records shall be automatically declassified no longer than 25 years from the date of its original classification, except as provided in paragraph (b), below.

(b) An agency head may exempt from automatic declassification under paragraph (a), above, specific information, the release of which should be expected to:

(1) reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the unauthorized disclosure of that source would clearly and demonstrably damage the national security interests of the United States;

(2) reveal information that would assist in the development or use of weapons of mass destruction;

(3) reveal information that would impair U.S. cryptologic systems or activities;

(4) reveal information that would impair the application of state of the art technology within a U.S. weapon system;

(5) reveal actual U.S. military war plans that remain in effect;

(6) reveal information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

(7) reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized;

(8) reveal information that would seriously and demonstrably impair current national security emergency preparedness plans; or

(9) violate a statute, treaty, or international agreement.

(c) No later than the effective date of this order, an agency head shall notify the President through the Assistant to the President for National Security Affairs of any specific file series of records for which a review or assessment has determined that the information within those file series almost invariably falls within one or more of the exemption categories listed in paragraph (b), above, and which the agency proposes to exempt from automatic declassification. The notification shall include:

(1) a description of the file series;

(2) an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and

(3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b), above, a specific date or event for declassification of the information. The President may direct the agency head not to exempt the file series or to declassify the information within that series at an earlier date than recommended.

(d) At least 180 days before information is automatically declassified under this section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as executive secretary of the Interagency Security Classification Appeals Panel, of any specific information beyond that included in a notification to the President under paragraph (c), above, that the agency proposes to exempt from automatic declassification. The notification shall include:

(1) a description of the information;

(2) an explanation of why the information is exempt from automatic declassification and must remain classified for a longer period of time; and

(3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b), above, a specific date or event for declassification of the

information. The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. The agency head may appeal such a decision to the President through the Assistant to the President for National Security Affairs. The information will remain classified while such an appeal is pending.

(e) No later than the effective date of this order, the agency head or senior agency official shall provide the Director of the Information Security Oversight Office with a plan for compliance with the requirements of this section, including the establishment of interim target dates. Each such plan shall include the requirement that the agency declassify at least 15 percent of the records affected by this section no later than 1 year from the effective date of this order, and similar commitments for subsequent years until the effective date for automatic declassification.

(f) Information exempted from automatic declassification under this section shall remain subject to the mandatory and systematic declassification review provisions of this order.

(g) The Secretary of State shall determine when the United States should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty or international agreement that requires the classification of information contained in records affected by this section for a period longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this section.

Sec. 3.5 *Systematic Declassification Review.*

(a) Each agency that has originated classified information under this order or its predecessors shall establish and conduct a program for systematic declassification review. This program shall apply to historically valuable records exempted from automatic declassification under section 3.4 of this order. Agencies shall prioritize the systematic review of records based upon:

(1) recommendations of the Information Security Policy Advisory Council, established in section 5.5 of this order, on specific subject areas for systematic review concentration; or

(2) the degree of researcher interest and the likelihood of declassification upon review.

(b) The Archivist shall conduct a systematic declassification review program for classified information: (1) accessioned into the National Archives as of the effective date of this order; (2) information transferred to the Archivist pursuant to section 2203 of title 44, United States Code; and (3) information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that has gone out of existence. This program shall apply to pertinent records no later than 25 years from the date of their creation. The Archivist shall establish priorities for the systematic review of these records based upon the recommendations of the Information Security Policy Advisory Council; or the degree of researcher interest and the likelihood of declassification upon review. These records shall be reviewed in accordance with the standards of this order, its implementing directives, and declassification guides provided to the Archivist by each agency that originated the records. The Director of the Information Security Oversight Office shall assure that agencies provide the Archivist with adequate and current declassification guides.

(c) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

Sec. 3.6 *Mandatory Declassification Review.*

(a) Except as provided in paragraph (b), below, all information classified under this order or predecessor orders shall be subject to a review for declassification by the originating agency if:

(1) the request for a review describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;

(2) the information is not exempted from search and review under the Central Intelligence Agency Information Act; and

(3) the information has not been reviewed for declassification within the past two years. If the agency has reviewed the information within the past two years, or the information is the subject of pending litigation, the agency shall inform the requester of this fact and of the requester's appeal rights.

(b) Information originated by

(1) the incumbent President;

(2) the incumbent President's White House Staff;

(3) committees, commissions, or boards appointed by the incumbent President; or

(4) other entities within the Executive Office of the President that solely advise and assist the incumbent President is exempted from the provisions of paragraph (a), above. However, the Archivist shall have the authority to review, downgrade, and declassify information of former presidents under the control of the Archivist pursuant to sections 2107, 2111, 2111 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective presidential papers or records. Agencies with primary subject matter interest shall be notified promptly of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Interagency Security Classification Appeals Panel. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under this order. They shall release this information unless withholding is otherwise authorized and warranted under applicable law.

(d) In accordance with directives issued pursuant to this order, agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They also shall provide a means for administratively appealing a denial of a mandatory review request,

and for notifying the requester of the right to appeal a final agency decision to the Interagency Security Classification Appeals Panel.

(e) After consultation with affected agencies, the Secretary of Defense shall develop special procedures for the review of cryptologic information, the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods, and the Archivist shall develop special procedures for the review of information accessioned into the National Archives.

Sec. 3.7 *Processing Requests and Reviews.*

In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this order, or pursuant to the automatic declassification or systematic review provisions of this order:

(a) An agency may refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classified under this order.

(b) When an agency receives any request for documents in its custody that contain information that was originally classified by another agency, or comes across such documents in the process of the automatic declassification or systematic review provisions of this order, it shall refer copies of any request and the pertinent documents to the originating agency for processing, and may, after consultation with the originating agency, inform any requester of the referral unless such association is itself classified under this order. In cases in which the originating agency determines in writing that a response under paragraph (a), above, is required, the referring agency shall respond to the requester in accordance with that paragraph.

Sec. 3.8 *Declassification Database.*

(a) The Archivist in conjunction with the Director of the Information Security Oversight Office and those agencies that originate classified information, shall establish a Government-wide database of information that has been declassified. The Archivist shall also explore other possible uses of technology to facilitate the declassification process.

(b) Agency heads shall fully cooperate with the Archivist in these efforts.

(c) Except as otherwise authorized and warranted by law, all declassified information contained within the database established under paragraph (a), above, shall be available to the public.

Part 4 - Safeguarding

Sec. 4.1 *Definitions.* For purposes of this order:

(a) "Safeguarding" means measures and controls that are prescribed to protect classified information.

(b) "Access" means the ability or opportunity to gain knowledge of classified information.

(c) "Need-to-know" means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(d) "Automated information system" means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

(e) "Integrity" means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

(f) "Network" means a system of two or more computers that can exchange data or information.

(g) "Telecommunications" means the preparation, transmission, or communication of information by electronic means.

(h) "Special access program" means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Sec. 4.2 *General Restrictions on Access.*

(a) A person may have access to classified information provided that:

(1) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee;

(2) the person has signed an approved nondisclosure agreement; and

(3) the person has a need-to-know the information.

(b) Classified information shall remain under the control of the originating agency or its successor in function. An agency shall not disclose information originally classified by another agency without its authorization. An official or employee leaving agency service may not remove classified information from the agency's control.

(c) Classified information may not be removed from official premises without proper authorization.

(d) Persons authorized to disseminate classified information outside the executive branch shall assure the protection of the information in a manner equivalent to that provided within the executive branch.

(e) Consistent with law, directives and regulation, an agency head or senior agency official shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information have controls that:

(1) prevent access by unauthorized persons; and

(2) ensure the integrity of the information.

(f) Consistent with law, directives and regulation, each agency head or senior agency official shall establish controls to ensure that classified information is used, processed, stored, reproduced,

transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

(g) Consistent with directives issued pursuant to this order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to United States "Confidential" information, including allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved nondisclosure agreement.

(h) Except as provided by statute or directives issued pursuant to this order, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information originated within that agency. For purposes of this section, the Department of Defense shall be considered one agency.

Sec. 4.3 *Distribution Controls.*

(a) Each agency shall establish controls over the distribution of classified information to assure that it is distributed only to organizations or individuals eligible for access who also have a need-to-know the information.

(b) Each agency shall update, at least annually, the automatic, routine, or recurring distribution of classified information that they distribute. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

Sec. 4.4 *Special Access Programs.*

(a) *Establishment of special access programs.* Unless otherwise authorized by the President, only the Secretaries of State, Defense and Energy, and the Director of Central Intelligence, or the principal deputy of each, may create a special access program. For special access programs pertaining to intelligence activities (including special activities, but not including military operational, strategic and tactical programs), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only upon a specific finding that:

(1) the vulnerability of, or threat to, specific information is exceptional; and

(2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed suffient to protect the information from unauthorized disclosure; or

(3) the program is required by statute.

(b) *Requirements and limitations.*

(1) Special access programs shall be limited to programs in which the number of persons who will have access ordinarily will be reasonably small and commensurate with the objective of providing enhanced protection for the information involved.

(2) Each agency head shall establish and maintain a system of accounting for special access programs consistent with directives issued pursuant to this order.

(3) Special access programs shall be subject to the oversight program established under section 5.6(c) of this order. In addition, the Director of the Information Security Oversight Office shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this order. An agency head may limit access to a special access program to the Director and no more than one other employee of the Information Security Oversight Office; or, for special access programs that are extraordinarily sensitive and vulnerable, to the Director only.

(4) The agency head or principal deputy shall review annually each special access program to determine whether it continues to meet the requirements of this order.

(5) Upon request, an agency shall brief the Assistant to the President for National Security Affairs, or his or her designee, on any or all of the agency's special access programs.

(c) Within 180 days after the effective date of this order, each agency head or principal deputy shall review all existing special access programs under the agency's jurisdiction. These officials shall terminate any special access programs that do not clearly meet the provisions of this order. Each existing special access program that an agency head or principal deputy validates shall be treated as if it were established on the effective date of this order.

(d) Nothing in this order shall supersede any requirement made by or under 10 U.S.C. 119.

Sec. 4.5 *Access by Historical Researchers and Former Presidential Appointees.*

(a) The requirement in section 4.2(a)(3) of this order that access to classified information may be granted only to individuals who have a need-to-know the information may be waived for persons who:

(1) are engaged in historical research projects; or

(2) previously have occupied policy-making positions to which they were appointed by the President.

(b) Waivers under this section may be granted only if the agency head or senior agency official of the originating agency:

(1) determines in writing that access is consistent with the interest of national security;

(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this order; and

(3) limits the access granted to former presidential appointees to items that the person originated, reviewed, signed, or received while serving as a presidential appointee.

Part 5 - Implementation and Review

Sec. 5.1 *Definitions.* For purposes of this order:

(a) "Self-inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.

(b) "Violation" means:

(1) any knowing, willful or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;

(2) any knowing, willful or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or

(3) any knowing, willful or negligent action to create or continue a special access program contrary to the requirements of this order.

(c) "Infraction" means any knowing, willful or negligent action contrary to the requirements of this order or its implementing directives that does not comprise a "violation," as defined above.

Sec. 5.2 *Program Direction.*

(a) The Director of the Office of Management and Budget, in consultation with the Assistant to the President for National Security Affairs and the co-chairs of the Security Policy Board, shall issue such directives as are necessary to implement this order. These directives shall be binding upon the agencies. Directives issued by the Director of the Office of Management and Budget shall establish standards for:

(1) classification and marking principles;

(2) agency security education and training programs;

(3) agency self-inspection programs; and

(4) classification and declassification guides.

(b) The Director of the Office of Management and Budget shall delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office.

(c) The Security Policy Board, established by a Presidential Decision Directive, shall make a recommendation to the President through the Assistant to the President for National Security Affairs with respect to the issuance of a Presidential directive on safeguarding classified information. The Presidential directive shall pertain to the handling, storage, distribution, transmittal and destruction of and accounting for classified information.

Sec. 5.3 *Information Security Oversight Office.*

(a) There is established within the Office of Management and Budget an Information Security Oversight Office. The Director of the Office of Management and Budget shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(b) Under the direction of the Director of the Office of Management and Budget acting in consultation with the Assistant to the President for National Security Affairs, the Director of the Information Security Oversight Office shall:

(1) develop directives for the implementation of this order;

(2) oversee agency actions to ensure compliance with this order and its implementing directives;

(3) review and approve agency implementing regulations and agency guides for systematic declassification review prior to their issuance by the agency;

(4) have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the Director of the Office of Management and Budget within 60 days of the request for access. Access shall be denied pending a prompt decision by the Director of the Office of Management and Budget, who shall consult on this decision with the Assistant to the President for National Security Affairs;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend presidential approval through the Director of the Office of Management and Budget;

(6) consider and take action on complaints and suggestions from persons within or outside the government with respect to the administration of the program established under this order;

(7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this order;

(8) report at least annually to the President on the implementation of this order; and

(9) convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

Sec. 5.4 *Interagency Security Classification Appeals Panel.*

(a) *Establishment and Administration.*

(1) There is established an Interagency Security Classification Appeals Panel ("Panel"). The Secretaries of State and Defense, the Attorney General, the Director of Central Intelligence, the Archivist of the United States, and the Assistant to the President for National Security Affairs shall each appoint a senior level representative to serve as a member of the Panel. The President shall select the Chair of the Panel from among the Panel members.

(2) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (1), above.

(3) The Director of the Information Security Oversight Office shall serve as the Executive Secretary. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel.

(4) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panel's functions.

(5) The Panel shall meet at the call of the Chair. The Chair shall schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner.

(6) The Information Security Oversight Office shall include in its reports to the President a summary of the Panel's activities.

(b) *Functions.* The Panel shall:

(1) decide on appeals by persons who have filed classification challenges under section 1.9 of this order;

(2) approve, deny or amend agency exemptions from automatic declassification as provided in section 3.4 of this order; and

(3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under section 3.6 of this order.

(c) *Rules and Procedures.* The Panel shall issue bylaws, which shall be published in the *Federal Register* no later than 120 days from the effective date of this order. The bylaws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that the Panel will consider appeals only on actions in which: (1) the appellant has exhausted his or her administrative remedies within the responsible agency; (2) there is no current action pending on the issue within the federal courts; and (3) the information has not been the subject of review by the federal courts or the Panel within the past two years.

(d) Agency heads will cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. An agency head may appeal a decision of the Panel to the President through the Assistant to the President for National Security Affairs. The Panel will report to the President through the Assistant to the President for National Security Affairs any instance in which it believes that an agency head is not cooperating fully with the Panel.

(e) The Appeals Panel is established for the sole purpose of advising and assisting the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States. Panel decisions are committed to the discretion of the Panel, unless reversed by the President.

Sec. 5.5 *Information Security Policy Advisory Council.*

(a) *Establishment.* There is established an Information Security Policy Advisory Council ("Council"). The Council shall be composed of seven members appointed by the President for staggered terms not to exceed four years, from among persons who have demonstrated interest and expertise in an area related to the subject matter of this order and are not otherwise employees of the Federal Government. The President shall appoint the Council chair from among the members. The Council shall comply with the Federal Advisory Committee Act, as amended, 5 U.S.C. App. 2.

(b) *Functions.* The Council shall:

(1) advise the President, the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, or such other executive branch officials as it deems appropriate, on policies established under this order or its implementing directives, including recommended changes to those policies;

(2) provide recommendations to agency heads for specific subject areas for systematic declassification review; and

(3) serve as a forum to discuss policy issues in dispute.

(c) *Meetings.* The Council shall meet at least twice each calendar year, and as determined by the Assistant to the President for National Security Affairs or the Director of the Office of Management and Budget.

(d) *Administration.*

(1) Each Council member may be compensated at a rate of pay not to exceed the daily equivalent of the annual rate of basic pay in effect for grade GS-18 of the general schedule under section 5376 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Council.

(2) While away from their homes or regular place of business in the actual performance of the duties of the Council, members may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government service (5 U.S.C. 5703(b)).

(3) To the extent permitted by law and subject to the availability of funds, the Information Security Oversight Office shall provide the Council with administrative services, facilities, staff, and other support services necessary for the performance of its functions.

(4) Notwithstanding any other Executive order, the functions of the President under the Federal Advisory Committee Act, as amended, that are applicable to the Council, except that of reporting to the Congress, shall be performed by the Director of the Information Security Oversight Office in accordance with the guidelines and procedures established by the General Services Administration.

Sec. 5.6 *General Responsibilities.*

Heads of agencies that originate or handle classified information shall:

(a) demonstrate personal commitment and commit senior management to the successful implementation of the program established under this order;

(b) commit necessary resources to the effective implementation of the program established under this order;

(c) designate a senior agency official to direct and administer the program, whose responsibilities shall include:

(1) overseeing the agency's program established under this order, provided, an agency head may designate a separate official to oversee special access programs authorized under this

order. This official shall provide a full accounting of the agency's special access programs at least annually;

(2) promulgating implementing regulations, which shall be published in the *Federal Register* to the extent that they affect members of the public;

(3) establishing and maintaining security education and training programs;

(4) establishing and maintaining an ongoing self-inspection program, which shall include the periodic review and assessment of the agency's classified product;

(5) establishing procedures to prevent unnecessary access to classified information, including procedures that: (i) require that a need for access to classified information is established before initiating administrative clearance procedures; and (ii) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs;

(6) developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

(7) assuring that the performance contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of: (i) original classification authorities; (ii) security managers or security specialists; and (iii) all other personnel whose duties significantly involve the creation or handling of classified information;

(8) accounting for the costs associated with the implementation of this order, which shall be reported to the Director of the Information Security Oversight Office for publication; and

(9) assigning in a prompt manner agency personnel to respond to any request, appeal, challenge, complaint or suggestion arising out of this order that pertains to classified information that originated in a component of the agency that no longer exists and for which there is no clear successor in function.

Sec. 5.7 *Sanctions.*

(a) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, certificate holders, and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:

(1) disclose to unauthorized persons information properly classified under this order or predecessor orders;

(2) classify or continue the classification of information in violation of this order or any implementing directive;

(3) create or continue a special access program contrary to the requirements of this order; or

(4) contravene any other provision of this order or its implementing directives.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this order.

(e) The agency head or senior agency official shall:

(1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b), above, occurs; and

(2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2) or (3), above, occurs.

Part 6 - General Provisions

Sec. 6.1 *General Provisions.*

(a) Nothing in this order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(c) Nothing in this order limits the protection afforded any information by other provisions of law, including the exemptions to the Freedom of Information Act, the Privacy Act, and the National Security Act of 1947, as amended. This order is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its agencies, its officers, or its employees. The foregoing is in addition to the specific provisos set forth in sections 1.2(b), 3.2(b) and 5.4(e) of this order.

(d) Executive Order No. 12356 of April 6, 1982, is revoked as of the effective date of this order.

Sec. 6.2 *Effective Date.*

This order shall become effective 180 days from the date of its issuance.

William J. Clinton

THE WHITE HOUSE
April 17, 1995

Implementing Directive
For
Executive Order 12958

"Classfied National Security Information"

32 CFR PART 2001

October 13, 1995

Table of Contents

Authority: Section 5.2(a) and (b), E.O. 12958, 60 FR 19825, April 20, 1995.

Subpart A - Classification

§2001.10 *Classification definitions and standards [Sec. 1.1 and 1.2]*[1]

(a) *Definitions.* (1) An *"original classification authority with jurisdiction over the information"* includes:

(i) The official who authorized the original classification, if that official is still serving in the same position;

(ii) The originator's current successor in function;

(iii) A supervisory official of either; or

(iv) The senior agency official under Executive Order 12958 ("the Order").

(2) *"Permanently valuable information"* or *"permanent historical value"* refers to information contained in:

(i) Records that have been accessioned into the National Archives of the United States;

(ii) Records that have been scheduled as permanent under a records retention schedule approved by the National Archives and Records Administration (NARA); and

(iii) Presidential historical materials, presidential records or donated historical materials located in the National Archives of the United States, a presidential library, or any other approved repository.

(b) *Identifying or describing damage to the national security.* Section 1.2(a) of the Order sets forth the conditions for classifying information in the first instance. One of these conditions, the ability to identify or describe the damage to the national security, is critical to the process of making an original classification decision. There is no requirement, at the time of the decision, for the original classification authority to prepare a written description of such damage. However, the original classification authority must be able to support the decision in writing, including identifying or describing the damage, should the classification decision become the subject of a challenge or access demand.

§2001.11 *Classification authority [1.4]*

(a) *General.* Agencies with original classification authority shall establish a training program for original classifiers in accordance with this part.

(b) *Requests for original classification authority.* Agencies not possessing such authority shall forward requests to the Director of the Information Security Oversight Office (ISOO). The agency head must make the request and shall provide a specific justification of the need for this authority. The Director of ISOO shall forward the request, along with the Director's

---

[1] Bracketed references pertain to related sections of Executive Order 12958.

recommendation, to the President through the Director of the Office of Management and Budget within 30 days. Agencies wishing to increase their assigned level of original classification authority shall forward requests in accordance with the procedures of this section.

§2001.12 *Duration of classification [1.6]*

(a) *Determining duration of classification for information originally classified under the Order.*

(1) *Establishing duration of classification.* When determining the duration of classification for information originally classified under this Order, an original classification authority shall follow the sequence listed in paragraphs (a)(1)(i), (ii), and (iii) of this section.

(i) The original classification authority shall attempt to determine a date or event that is less than 10 years from the date of original classification and which coincides with the lapse of the information's national security sensitivity, and shall assign such date or event as the declassification instruction.

(ii) If unable to determine a date or event of less than 10 years, the original classification authority shall ordinarily assign a declassification date that is 10 years from the date of the original classification decision.

(iii) The original classification authority may assign an exemption designation to the information only if the information qualifies for exemption from automatic declassification as described in section 1.6(d) of the Order. Unless declassified earlier, such information contained in records determined by the Archivist of the United States to be permanently valuable shall remain classified for 25 years from the date of its origin, at which time it will be subject to section 3.4 of the Order.

(2) *Extending duration of classification for information originally classified under the Order.* Extensions of classification are not automatic. If an original classification authority with jurisdiction over the information does not extend the classification of information assigned a date or event for declassification, the information is automatically declassified upon the occurrence of the date or event. If an original classification authority has assigned a date or event for declassification that is 10 years or less from the date of classification, an original classification authority with jurisdiction over the information may extend the classification duration of such information for additional periods not to exceed 10 years at a time.

(i) For information in records determined to have permanent historical value, successive extensions may not exceed a total of 25 years from the date of the information's origin. Continued classification of this information beyond 25 years is governed by section 3.4 of the Order.

(ii) For information in records not determined to have permanent historical value, successive extensions may exceed 25 years from the date of the information's origin.

(3) *Conditions for extending classification.* When extending the duration of classification, the original classification authority must:

(i) Be an original classification authority with jurisdiction over the information;

(ii) Ensure that the information continues to meet the standards for classification under the Order; and

(iii) Make reasonable attempts to notify all known holders of the information.

(b) *Information classified under prior orders.*

(1) *Specific date or event.* Unless declassified earlier, information marked with a specific date or event for declassification under a prior order is automatically declassified upon that date or event. However, if the information is contained in records determined by the Archivist of the United States to be permanently valuable, and the prescribed date or event will take place more than 25 years from the information's origin, the declassification of the information will instead be subject to section 3.4 of the Order.

(2) *Indefinite duration of classification.* For information marked "Originating Agency's Determination Required," its acronym "OADR," or with some other marking indicating an indefinite duration of classification under a prior order:

(i) A declassification authority, as defined in section 3.1 of the Order, may declassify it;

(ii) An authorized original classification authority with jurisdiction over the information may re-mark the information to establish a duration of classification consistent with the requirements for information originally classified under the Order, as provided in paragraph (a) of this section; or

(iii) Unless declassified earlier, such information contained in records determined by the Archivist of the United States to be permanently valuable shall remain classified for 25 years from the date of its origin, at which time it will be subject to section 3.4 of the Order.

(c) *Foreign government information.* The declassifying agency is the agency that initially received or classified the information. When foreign government information is being considered for declassification or appears to be subject to automatic declassification, the declassifying agency shall determine whether the information is subject to a treaty or international agreement that would prevent its declassification at that time. Depending on the age of the information and whether it is contained in permanently valuable records, the declassifying agency shall also determine if another exemption under section 1.6(d) (other than section 1.6(d)(5)) or 3.4(b) of the Order, such as the exemptions that pertain to United States foreign relations, may apply to the information. If the declassifying agency believes such an exemption may apply, it should consult with any other concerned agencies in making its declassification determination. The declassifying agency or the Department of State, as appropriate, should consult with the foreign government prior to declassification.

(d) *Determining when information is subject to automatic declassification.* The "date of the information's origin" or "the information's origin," as used in the Order and this part, pertains to the date that specific information, which is contemporaneously or subsequently classified, is first recorded in an agency's records, or in presidential historical materials, presidential records or donated historical materials. The following examples illustrate this process:

Example 1: An agency first issues a classification guide on the F-99 aircraft on October 20, 1995. The guide states that the fact that the F-99 aircraft has a maximum velocity of

500 m.p.h. shall be classified at the "Secret" level for a period of ten years. A document dated July 10, 1999, is classified because it includes the maximum velocity of the F-99. The document should be marked for declassification on October 20, 2005, ten years after the specific information was first recorded in the guide, not on July 10, 2009, ten years after the derivatively classified document was created.

Example 2: An agency classification guide issued on October 20, 1995, states that the maximum velocity of any fighter aircraft shall be classified at the "Secret" level for a period of ten years. The agency first records the specific maximum velocity of the new F-88 aircraft on July 10, 1999. The document should be marked for declassification on July 10, 2009, ten years after the specific information is first recorded, and not on October 20, 2005, ten years after the date of the guide's generic instruction.

§2001.13 *Classification challenges [1.9]*

(a) *Challenging classification.* Authorized holders wishing to challenge the classification status of information shall present such challenges to an original classification authority with jurisdiction over the information. An authorized holder is any individual, including an individual external to the agency, who has been granted access to specific classified information in accordance with section 4.2(g) of the Order. A formal challenge under this provision must be in writing, but need not be any more specific than to question why information is or is not classified, or is classified at a certain level.

(b) *Agency procedures.* (1) Because the Order encourages authorized holders to challenge classification as a means for promoting proper and thoughtful classification actions, agencies shall ensure that no retribution is taken against any authorized holders bringing such a challenge in good faith.

(2) Agencies shall establish a system for processing, tracking and recording formal classification challenges made by authorized holders. Agencies shall consider classification challenges separately from Freedom of Information Act or other access requests, and shall not process such challenges in turn with pending access requests.

(3) The agency shall provide an initial written response to a challenge within 60 days. If the agency is unable to respond to the challenge within 60 days, the agency must acknowledge the challenge in writing, and provide a date by which the agency will respond. The acknowledgment must include a statement that if no agency response is received within 120 days, the challenger has the right to forward the challenge to the Interagency Security Classification Appeals Panel for a decision. The challenger may also forward the challenge to the Interagency Security Classification Appeals Panel if an agency has not responded to an internal appeal within 90 days of the agency's receipt of the appeal. Agency responses to those challenges it denies shall include the challenger's appeal rights to the Interagency Security Classification Appeals Panel.

(4) Whenever an agency receives a classification challenge to information that has been the subject of a challenge within the past two years, or that is the subject of pending litigation, the agency is not required to process the challenge beyond informing the challenger of this fact and of the challenger's appeal rights, if any.

(c) *Additional considerations.* (1) Challengers and agencies shall attempt to keep all challenges, appeals and responses unclassified. However, classified information contained in a challenge, an agency response, or an appeal shall be handled and protected in accordance with the Order and its implementing directives. Information being challenged for classification shall remain classified unless and until a final decision is made to declassify it.

(2) The classification challenge provision is not intended to prevent an authorized holder from informally questioning the classification status of particular information. Such informal inquiries should be encouraged as a means of holding down the number of formal challenges.

§2001.14 *Classification guides [2.3]*

(a) *Preparation of classification guides.* Originators of classification guides are encouraged to consult users of guides for input when developing or updating guides. When possible, originators of classification guides are encouraged to communicate within their agencies and with other agencies that are developing guidelines for similar activities to ensure the consistency and uniformity of classification decisions. Each agency shall maintain a list of its classification guides in use.

(b) *General content of classification guides.* Classification guides shall, at a minimum:

(1) Identify the subject matter of the classification guide;

(2) Identify the original classification authority by name or personal identifier, and position;

(3) Identify an agency point-of-contact or points-of-contact for questions regarding the classification guide;

(4) Provide the date of issuance or last review;

(5) State precisely the elements of information to be protected;

(6) State which classification level applies to each element of information, and, when useful, specify the elements of information that are unclassified;

(7) State, when applicable, special handling caveats;

(8) Prescribe declassification instructions or the exemption category from automatic declassification for each element of information;

(9) Specify, when citing the exemption category listed in section 1.6(d)(8) of the Order, the applicable statute, treaty or international agreement; and

(10) State a concise reason for classification which, at a minimum, cites the applicable classification category or categories in section 1.5 of the Order.

(c) *Dissemination of classification guides.* Classification guides shall be disseminated as widely as necessary to ensure the proper and uniform derivative classification of information.

(d) *Reviewing and updating classification guides.* (1) Classification guides, including guides created under prior orders, shall be reviewed and updated as circumstances require, but, in any event, at least once every five years. Updated instructions for guides first created under prior orders shall comply with the requirements of the Order and this part.

(2) Originators of classification guides are encouraged to consult the users of guides for input when reviewing or updating guides. Also, users of classification guides are encouraged to notify the originator of the guide when they acquire information that suggests the need for change in the instructions contained in the guide.

Subpart B - Identification and Markings

§2001.20 *General [1.7]*

A uniform security classification system requires that standard markings be applied to classified information. Except in extraordinary circumstances, or as approved by the Director of ISOO, the marking of classified information created after October 14, 1995, shall not deviate from the following prescribed formats. If markings cannot be affixed to specific classified information or materials, the originator shall provide holders or recipients of the information with written instructions for protecting the information. Markings shall be uniformly and conspicuously applied to leave no doubt about the classified status of the information, the level of protection required, and the duration of classification.

§2001.21 *Original classification [1.7(a)]*

(a) *Primary markings.* On the face of each originally classified document, including electronic media, the classifier shall apply the following markings.

(1) *Classification authority.* The name or personal identifier, and position title of the original classifier shall appear on the "Classified By" line. An example might appear as:

Classified By: David Smith, Chief, Division 5
or
Classified By: ID#IMNO1, Chief, Division 5

(2) *Agency and office of origin.* If not otherwise evident, the agency and office of origin shall be identified and placed below the name on the "Classified By" line. An example might appear as:

Classified By: David Smith, Chief, Division 5
Department of Good Works, Office of Administration

(3) *Reason for classification.* The original classifier shall identify the reason(s) for the decision to classify. The classifier shall include, at a minimum, a brief reference to the pertinent classification category(ies), or the number 1.5 plus the letter(s) that corresponds to that classification category in section 1.5 of the Order.

(i) These categories, as they appear in the Order, as follows:

(a) military plans, weapons, or operations;

(b) foreign government information;

(c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;

(d) foreign relations or foreign activities of the United States, including confidential sources;

(e) scientific, technological, or economic matters relating to the national security;

(f) United States Government programs for safeguarding nuclear materials or facilities; or

(g) vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

(ii) An example might appear as:

Classified By: David Smith, Chief, Division 5
Department of Good Works, Office of Administration
Reason: Vulnerabilities or capabilities of plans relating to the national security
or
Reason: 1.5(g)

(iii) When the reason for classification is not apparent from the content of the information, e.g., classification by compilation, the classifier shall provide a more detailed explanation of the reason for classification.

(4) *Declassification instructions.* The duration of the original classification decision shall be placed on the "Declassify On" line. The classifier will apply one of the following instructions.

(i) The classifier will apply a date or event for declassification that corresponds to the lapse of the information's national security sensitivity, which may not exceed 10 years from the date of the original decision. When linking the duration of classification to a specific date or event, mark that date or event as:

Classified By: David Smith, Chief, Division 5
Department of Good Works, Office of Administration
Reason: 1.5(g)
Declassify On: October 14, 2004
or
Declassify On: Completion of Operation

(ii) When a specific date or event within 10 years cannot be established, the classifier will apply the date that is 10 years from the date of the original decision. For example, on a document that contains information classified on October 14, 1995, mark the "Declassify On" line as:

Classified By: David Smith, Chief, Division 5
Department of Good Works, Office of Administration
Reason: 1.5(g)
Declassify On: October 14, 2005

(iii) Upon the determination that the information must remain classified beyond 10 years, the classifier will apply the letter "X" plus a brief recitation of the exemption

category(ies), or the letter "X" plus the number that corresponds to that exemption category(ies) in section 1.6(d) of the Order.

(A) *Exemption categories in E.O. 12958.*

X1: reveal an intelligence source, method, or activity, or a cryptologic system or activity;
X2: reveal information that would assist in the development or use of weapons of mass destruction;
X3: reveal information that would impair the development or use of technology within a United States weapons system;
X4: reveal United States military plans, or national security emergency preparedness plans;
X5: reveal foreign government information;
X6: damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than that provided in paragraph (b), above, [section 1.5(b) of the Order];
X7: impair the ability of responsible United States Government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized; or
X8: violate a statute, treaty, or international agreement.

(B) *Example.* A document containing information exempted from automatic declassification may appear as:

Classified By: David Smith, Chief, Division 5
Department of Good Works, Office of Administration
Reason: 1.5(g)
Declassify On: X-U.S. military plans
or
Declassify On: X4

(b) *Overall marking.* The highest level of classified information contained in a document shall appear in a way that will distinguish it clearly from the informational text.

(1) Conspicuously place the overall classification at the top and bottom of the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any).

(2) For documents containing information classified at more than one level, the overall marking shall be the highest level. For example, if a document contains some information marked "Secret" and other information marked "Confidential," the overall marking would be "Secret."

(3) Each interior page of a classified document shall be marked at the top and bottom either with the highest level of classification of information contained on that page, including the designation "Unclassified" when it is applicable, or with the highest overall classification of the document.

(c) *Portion marking.* Each portion of a document, ordinarily a paragraph, but including subjects, titles, graphics and the like, shall be marked to indicate its classification level by placing a parenthetical symbol immediately preceding or following the portion to which it applies.

(1) To indicate the appropriate classification level, the symbols "(TS)" for Top Secret, "(S)" for Secret, "(C)" for Confidential, and "(U)" for Unclassified shall be used.

(2) Unless the original classification authority indicates otherwise on the document, each classified portion of a document exempted from automatic declassification shall be presumed to be exempted from automatic declassification also.

(3) An agency head or senior agency official may request a waiver from the portion marking requirement for a specific category of information. Such a request shall be submitted to the Director of ISOO and should include the reasons that the benefits of portion marking are outweighed by other factors. Statements citing administrative burden alone will ordinarily not be viewed as sufficient grounds to support a waiver.

(d) *Classification extensions.* (1) An original classification authority may extend the duration of classification for successive periods not to exceed 10 years at a time. For information contained in records determined to be permanently valuable, multiple extensions shall not exceed 25 years from the date of the information's origin.

(2) The "Declassify On" line shall be revised to include the new declassification instructions, and shall include the identity of the person authorizing the extension and the date of the action.

(3) The office of origin shall make reasonable attempts to notify all holders of such information. Classification guides shall be updated to reflect such revisions.

(4) An example of an extended duration of classification may appear as:

Classified By: David Smith, Chief, Division 5
Department of Good Works, Office of Administration
Reason: 1.5(g)
Declassify On: Classification extended on December 1, 2000
until December 1, 2010, by David Jones, Chief, Division 5

(e) *Marking information exempted from automatic declassification at 25 years.* (1) When an agency head or senior agency official exempts permanently valuable information from automatic declassification at 25 years, the "Declassify On" line shall be revised to include the symbol "25X" plus a brief reference to the pertinent exemption category(ies) or the number(s) that corresponds to that category(ies) in section 3.4(b) of the Order. Other than when the exemption pertains to the identity of a confidential human source, or a human intelligence source, the revised "Declassify On" line shall also include the new date or event for declassification.

(2) The pertinent exemptions, using the language of section 3.4(b) of the Order, are:

25X1: reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the unauthorized disclosure of that source would clearly and demonstrably damage the national security interests of the United States;

25X2: reveal information that would assist in the development or use of weapons of mass destruction;
25X3: reveal information that would impair U.S. cryptologic systems or activities;
25X4: reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system;
25X5: reveal actual U.S. military war plans that remain in effect;
25X6: reveal information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;
25X7: reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized;
25X8: reveal information that would seriously and demonstrably impair current national security emergency preparedness plans; or
25X9: violate a statute, treaty, or international agreement.

(3) The pertinent portion of the marking would appear as:

Declassify On: 25X-State-of-the-art technology within U.S. weapon system
October 1, 2010
or
Declassify On: 25X4
October 1, 2010

(4) Documents should not be marked with a "25X" marking until the agency has been informed that the President or the Interagency Security Classification Appeals Panel concurs with the proposed exemption.

(5) Agencies need not apply a "25X" marking to individual documents contained in a file series exempted from automatic declassification under section 3.4(c) of the Order until the individual document is removed from the file.

§2001.22 *Derivative classification [2.2]*

(a) *General.* Information classified derivatively on the basis of source documents or classification guides shall bear all markings prescribed in 2001.20 and 2001.21, except as provided in this section. Information for these markings shall be carried forward from the source document or taken from instructions in the appropriate classification guide.

(b) *Source of derivative classification.* (1) The derivative classifier shall concisely identify the source document or the classification guide on the "Derived From" line, including the agency and, where available, the office of origin, and the date of the source or guide. An example might appear as:

Derived From: Memo, "Funding Problems," October 20, 1995,
Ofc. of Admin., Department of Good Works
or
Derived From: CG No. 1, Department of Good Works, dated October 20

(i) When a document is classified derivatively on the basis of more than one source document or classification guide, the "Derived From" line shall appear as:

Derived From: Multiple Sources

(ii) The derivative classifier shall maintain the identification of each source with the file or record copy of the derivatively classified document. When practicable, this list should be included in or with all copies of the derivatively classified document.

(2) A document derivatively classified on the basis of a source document that is itself marked "Multiple Sources" shall cite the source document on its "Derived From" line rather than the term "Multiple Sources." An example might appear as:

Derived From: Report entitled, "New Weapons," dated October 20, 1995,
Department of Good Works, Office of Administration

(c) *Reason for classification.* The reason for the original classification decision, as reflected in the source document(s) or classification guide, is not required to be transferred in a derivative classification action. If included, however, it shall conform to the standards in 2001.21(a)(3).

(d) *Declassification instructions.* (1) The derivative classifier shall carry forward the instructions on the "Declassify On" line from the source document to the derivative document, or the duration instruction from the classification guide.

(2) When a document is classified derivatively on the basis of more than one source document or more than one element of a classification guide, the "Declassify On" line shall reflect the longest duration of any of its sources.

(i) When a document is classified derivatively from a source document(s) or classification guide that contains the declassification instruction, "Originating Agency's Determination Required," or "OADR," unless otherwise instructed by the original classifier, the derivative classifier shall carry forward:

(A) The fact that the source document(s) was marked with this instruction; and

(B) The date of origin of the most recent source document(s), classification guide, or specific information, as appropriate to the circumstances.

(ii) An example might appear as:

Declassify On: Source marked "OADR"
Date of source: October 20, 1990

(iii) This marking will permit the determination of when the classified information is 25 years old and, if permanently valuable, subject to automatic declassification under section 3.4 of the Order.

(e) *Overall marking.* The derivative classifier shall conspicuously mark the classified document with the highest level of classification of information included in the document, as provided in 2001.21(b).

(f) *Portion marking.* Each portion of a derivatively classified document shall be marked in accordance with its source, and as provided in 2001.21(c).

§2001.23 *Additional requirements [1.7]*

(a) *Marking prohibitions.* Markings other than "Top Secret," "Secret," and "Confidential," such as "For Official Use Only," or "Limited Official Use," shall not be used to identify classified national security information. No other term or phrase shall be used in conjunction with these markings, such as "Secret Sensitive" or "Agency Confidential," to identify classified national security information. The terms "Top Secret," "Secret," and "Confidential" should not be used to identify non-classified executive branch information.

(b) *Agency prescribed special markings.* Agencies shall refrain from the use of special markings when they merely restate or emphasize the principles and standards of the Order and this part. Upon request, the senior agency official shall provide the Director of ISOO with a written explanation for the use of agency special markings.

(c) *Transmittal documents.* A transmittal document shall indicate on its face the highest classification level of any classified information attached or enclosed. The transmittal shall also include conspicuously on its face the following or similar instructions, as appropriate:

UNCLASSIFIED WHEN CLASSIFIED ENCLOSURE REMOVED

or

UPON REMOVAL OF ATTACHMENTS, THIS DOCUMENT IS (CLASSIFICATION LEVEL)

(d) *Foreign government information.* Documents that contain foreign government information shall include the marking, "This Document Contains (indicate country of origin) Information." The portions of the document that contain the foreign government information shall be marked to indicate the government and classification level, e.g., "(UK-C)." If the identity of the specific government must be concealed, the document shall be marked, "This Document Contains Foreign Government Information," and pertinent portions shall be marked "FGI" together with the classification level, e.g., "(FGI-C)." In such cases, a separate record that identifies the foreign government shall be maintained in order to facilitate subsequent declassification actions. When classified records are transferred to the National Archives and Records Administration for storage or archival purposes, the accompanying documentation shall, at a minimum, identify the boxes that contain foreign government information. If the fact that information is foreign government information must be concealed, the markings described in this paragraph shall not be used and the document shall be marked as if it were wholly of U.S. origin.

(e) *Working papers.* A working paper is defined as documents or materials, regardless of the media, which are expected to be revised prior to the preparation of a finished product for dissemination or retention. Working papers containing classified information shall be dated when created, marked with the highest classification of any information contained in them, protected at that level, and destroyed when no longer needed. When any of the following conditions applies, working papers shall be controlled and marked in the same manner prescribed for a finished document at the same classification level:

(1) Released by the originator outside the originating activity;

(2) Retained more than 180 days from the date of origin; or

(3) Filed permanently.

(f) *Other material.* Bulky material, equipment and facilities, etc., shall be clearly identified in a manner that leaves no doubt about the classification status of the material, the level of protection required, and the duration of classification. Upon a finding that identification would itself reveal classified information, such identification is not required. Supporting documentation for such a finding must be maintained in the appropriate security facility and in any applicable classification guide.

(g) *Unmarked materials.* Information contained in unmarked records, or presidential or related materials, and which pertains to the national defense or foreign relations of the United States and has been maintained and protected as classified information under prior orders shall continue to be treated as classified information under the Order, and is subject to its provisions regarding declassification.

§2001.24 *Declassification markings*

[RESERVED]

Subpart C - Self-Inspections

§2001.30 *General [5.6]*

(a) *Purpose.* This subpart sets standards for establishing and maintaining an ongoing agency self-inspection program, which shall include the periodic review and assessment of the agency's classified product. "Self-inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under the Order.

(b) *Applicability.* These standards are binding on all executive branch agencies that create or handle classified information. Pursuant to Executive Order 12829, the *National Industrial Security Program Operating Manual* (NISPOM) prescribes the security requirements, restrictions and safeguards applicable to industry, including the conduct of contractor self-inspections. The standards established in the NISPOM should be consistent with the standards prescribed in Executive Order 12958 and this part.

(c) *Responsibility.* The senior agency official is responsible for the agency's self-inspection program. The senior agency official shall designate agency personnel to assist in carrying out this responsibility.

(d) *Approach.* The official(s) responsible for the program shall determine the means and methods for the conduct of self-inspections. These may include:

(1) A review of relevant security directives, guides and instructions;

(2) Interviews with producers and users of classified information;

(3) A review of access and control records and procedures; and

(4) A review of a sample of classified documents generated by agency activities.

(e) *Frequency.* The official(s) responsible for the program shall set the frequency of self-inspections on the basis of program needs and the degree of classification activity. Activities that originate

significant amounts of classified information should conduct at least one document review per year.

(f) *Reporting.* The format for documenting findings shall be set by the official(s) responsible for the program.

§2001.31 *Coverage [5.6(c)(4)]*

(a) *General.* These standards are not all-inclusive. Each agency may expand upon the coverage according to program and policy needs. Each self-inspection of an agency activity need not include all the elements covered in this section. Agencies without original classification authority need not include in their self-inspections those elements of coverage pertaining to original classification.

(b) *Elements of coverage.*

(1) *Original classification.*

(i) Evaluate original classifiers' general understanding of the process of original classification, including the:

(A) Applicable standards for classification;

(B) Levels of classification and the damage criteria associated with each; and

(C) Required classification markings.

(ii) Determine if delegations of original classification authority conform with the requirements of the Order, including whether:

(A) Delegations are limited to the minimum required to administer the program;

(B) Designated original classifiers have a demonstrable and continuing need to exercise this authority;

(C) Delegations are in writing and identify the official by name or position title; and

(D) New requests for delegation of classification authority are justified.

(iii) Assess original classifiers' familiarity with the duration of classification requirements, including:

(A) Assigning a specific date or event for declassification when possible;

(B) Establishing ordinarily a maximum 10-year duration of classification when an earlier date or event cannot be determined;

(C) Limiting extensions of classification for specific information for successive periods not to exceed 10 years at a time; and

(D) Exempting from declassification within 10 years specific information as provided in section 1.6 of the Order.

(iv) Conduct a review of a sample of classified information generated by the inspected activity to determine the propriety of classification and the application of proper and full markings.

(v) Evaluate classifiers' actions to comply with the standards specified in 2001.14 and 2001.53 of this part, relating to classification and declassification guides, respectively.

(vi) Verify observance with the prohibitions on classification and limitations on reclassification.

(vii) Assess whether the agency's classification challenges program meets the requirements of the Order and this part.

(2) *Derivative classification.* Assess the general familiarity of individuals who classify derivatively with the:

(i) Conditions for derivative classification;

(ii) Requirement to consult with the originator of the information when questions concerning classification arise;

(iii) Proper use of classification guides; and

(iv) Proper and complete application of classification markings to derivatively classified documents.

(3) *Declassification.*

(i) Verify whether the agency has established, to the extent practical, a system of records management to facilitate public release of declassified documents.

(ii) Evaluate the status of the agency declassification program, including the requirement to:

(A) Comply with the automatic declassification provisions regarding historically valuable records over 25 years old;

(B) Declassify, when possible, historically valuable records prior to accession into the National Archives;

(C) Provide the Archivist with adequate and current declassification guides;

(D) Ascertain that the agency's mandatory review program conforms to established requirements; and

(E) Determine whether responsible agency officials are cooperating with the Archivist in the development and maintenance of a Government-wide database of information that has been declassified.

(4) *Safeguarding.*

(i) Monitor agency adherence to established safeguarding standards.

(ii) Assess compliance with controls for access to classified information.

(iii) Evaluate the effectiveness of the agency's program in detecting and processing security violations and preventing recurrences.

(iv) Assess compliance with the procedures for identifying, reporting and processing unauthorized disclosures of classified information.

(v) Evaluate the effectiveness of procedures to ensure that:

(A) The originating agency exercises control over the classified information it generates;

(B) Holders of classified information do not disclose information originated by another agency without that agency's authorization; and

(C) Departing or transferred officials return all classified information in their possession to authorized agency personnel.

(5) *Security education and training.* Evaluate the effectiveness of the agency's security education and training program in familiarizing appropriate personnel with classification procedures; and determine whether the program meets the standards specified in subpart D of this part.

(6) *Management and oversight.*

(i) Determine whether original classifiers have received prescribed training.

(ii) Verify whether the agency's special access programs:

(A) Adhere to specified criteria in the creation of these programs;

(B) Are kept to a minimum;

(C) Provide for the conduct of internal oversight; and

(D) Include an annual review of each program to determine whether it continues to meet the requirements of the Order.

(iii) Assess whether:

(A) Senior management demonstrates commitment to the success of the program, including providing the necessary resources for effective implementation;

(B) Producers and users of classified information receive guidance with respect to security responsibilities and requirements;

(C) Controls to prevent unauthorized access to classified information are effective;

(D) Contingency plans are in place for safeguarding classified information used in or near hostile areas;

(E) The performance contract or other system used to rate civilian or military personnel includes the management of classified information as a critical element or item to be evaluated in the rating of: Original classifiers; security managers; classification management officers; and security specialists; and other employees significantly involved with classified information; and

(F) A method is in place for collecting information on the costs associated with the implementation of the Order.

Subpart D - Security Education and Training

§2001.40 *General [5.6]*

(a) *Purpose.* This subpart sets standards for agency security education and training programs. Implementation of these standards should:

(1) Ensure that all executive branch employees who create, process or handle classified information have a satisfactory knowledge and understanding about classification, safeguarding, and declassification policies and procedures;

(2) Increase uniformity in the conduct of agency security education and training programs; and

(3) Reduce improper classification, safeguarding and declassification practices.

(b) *Applicability.* These standards are binding on all executive branch departments and agencies that create or handle classified information. Pursuant to Executive Order 12829, the NISPOM prescribes the security requirements, restrictions, and safeguards applicable to industry, including the conduct of contractor security education and training. The standards established in the NISPOM should be consistent with the standards prescribed in Executive Order 12958 and of this part.

(c) *Responsibility.* The senior agency official is responsible for the agency's security education and training program. The senior agency official shall designate agency personnel to assist in carrying out this responsibility.

(d) *Approach.* Security education and training should be tailored to meet the specific needs of the agency's security program, and the specific roles employees are expected to play in that program. The agency official(s) responsible for the program shall determine the means and methods for providing security education and training. Training methods may include briefings, interactive videos, dissemination of instructional materials, and other media and methods. Agencies shall maintain records about the programs it has offered and employee participation in them.

(e) *Frequency.* The frequency of agency security education and training will vary in accordance with the needs of the agency's security classification program. Each agency shall provide some form of refresher security education and training at least annually.

§2001.41 *Coverage [5.6(c)(3)]*

(a) *General.* Each department or agency shall establish and maintain a formal security education and training program which provides for initial and refresher training, and termination briefings. This subpart establishes security education and training standards for original classifiers, declassification authorities, security managers, classification management officers, security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information. These standards are not intended to be all-inclusive. The official responsible for the security education and training program may expand or modify the coverage provided in this part according to the agency's program and policy needs.

(b) *Elements of initial coverage.* All cleared agency personnel shall receive initial training on basic security policies, principles and practices. Such training must be provided in conjunction with the granting of a security clearance, and prior to granting access to classified information. The following areas should be considered for inclusion in initial briefings.

(1) *Roles and responsibilities.*

(i) What are the responsibilities of the senior agency official, classification management officers, the security manager and the security specialist?

(ii) What are the responsibilities of agency employees who create or handle classified information?

(iii) Who should be contacted in case of questions or concerns about classification matters?

(2) *Elements of classifying and declassifying information.*

(i) What is classified information and why is it important to protect it?

(ii) What are the levels of classified information and the damage criteria associated with each level?

(iii) What are the prescribed classification markings and why is it important to have classified information fully and properly marked?

(iv) What are the general requirements for declassifying information?

(v) What are the procedures for challenging the classification status of information?

(3) *Elements of safeguarding.*

(i) What are the proper procedures for safeguarding classified information?

(ii) What constitutes an unauthorized disclosure and what are the penalties associated with these disclosures?

(iii) What are the general conditions and restrictions for access to classified information?

(iv) What should an individual do when he or she believes safeguarding standards may have been violated?

(c) *Specialized security education and training.* Original classifiers, authorized declassification authorities, individuals specifically designated as responsible for derivative classification, classification management officers, security managers, security specialists, and all other personnel whose duties significantly involve the creation or handling of classified information should receive more detailed training. This training should be provided before or concurrent with the date the employee assumes any of the positions listed above, but in any event no later than six months from that date. Coverage considerations should include:

(1) *Original classifiers.*

(i) What is the difference between original and derivative classification?

(ii) Who can classify information originally?

(iii) What are the standards that a designated classifier must meet to classify information?

(iv) What is the process for determining duration of classification?

(v) What are the prohibitions and limitations on classifying information?

(vi) What are the basic markings that must appear on classified information?

(vii) What are the general standards and procedures for declassification?

(2) *Declassification authorities other than original classifiers.*

(i) What are the standards, methods and procedures for declassifying information under Executive Order 12958?

(ii) What are the standards for creating and using agency declassification guides?

(iii) What is contained in the agency's automatic declassification plan?

(iv) What are the agency responsibilities for the establishment and maintenance of a declassification database?

(3) *Individuals specifically designated as responsible for derivative classification, security managers, classification management officers, security specialists or any other personnel whose duties significantly involve the management and oversight of classified information.*

(i) What are the original and derivative classification processes and the standards applicable to each?

(ii) What are the proper and complete classification markings, as described in subpart B of this part?

(iii) What are the authorities, methods and processes for downgrading and declassifying information?

(iv) What are the methods for the proper use, storage, reproduction, transmission, dissemination and destruction of classified information?

(v) What are the requirements for creating and updating classification and declassification guides?

(vi) What are the requirements for controlling access to classified information?

(vii) What are the procedures for investigating and reporting instances of security violations, and the penalties associated with such violations?

(viii) What are the requirements for creating, maintaining, and terminating special access programs, and the mechanisms for monitoring such programs?

(ix) What are the procedures for the secure use, certification and accreditation of automated information systems and networks which use, process, store, reproduce, or transmit classified information?

(x) What are the requirements for oversight of the security classification program, including agency self-inspections?

(d) *Refresher security education and training.* Agencies shall provide refresher training to employees who create, process or handle classified information. Refresher training should reinforce the policies, principles and procedures covered in initial and specialized training. Refresher training should also address the threat and the techniques employed by foreign intelligence activities attempting to obtain classified information, and advise personnel of penalties for engaging in espionage activities. Refresher training should also address issues or concerns identified during

agency self-inspections. When other methods are impractical, agencies may satisfy the requirement for refresher training by means of audiovisual products or written materials.

(e) *Termination briefings.* Each agency shall ensure that each employee granted access to classified information who leaves the service of the agency receives a termination briefing. Also, each agency employee whose clearance is withdrawn must receive such a briefing. At a minimum, termination briefings must impress upon each employee: The continuing responsibility not to disclose any classified information to which the employee had access and the potential penalties for non-compliance; and the obligation to return to the appropriate agency official all classified documents and materials in the employee's possession.

(f) *Other security education and training.* Agencies are encouraged to develop additional security education and training according to program and policy needs. Such security education and training could include:

(1) Practices applicable to U.S. officials traveling overseas;

(2) Procedures for protecting classified information processed and stored in automated information systems;

(3) Methods for dealing with uncleared personnel who work in proximity to classified information;

(4) Responsibilities of personnel serving as couriers of classified information; and

(5) Security requirements that govern participation in international programs.

Subpart E - Declassification

§2001.50 *Definition [3.1]*

A *"file series"* is a body of related records created or maintained by an agency, activity, office or individual. The records may be related by subject, topic, form, function, or filing scheme. An agency, activity, office, or individual may create or maintain several different file series, each serving a different function. Examples may include a subject file, alphabetical name index, chronological file, or a record set of agency publications. File series frequently correspond to items on a NARA-approved agency records schedule. Some very large series may contain several identifiable sub-series, and it may be appropriate to treat sub-series as discrete series for the purposes of the Order.

§2001.51 *Automatic declassification [3.4]*

(a) *General.* All departments and agencies that have original classification authority, or previously had original classification authority, and maintain records appraised as having permanent historical value that contain information classified by that agency shall comply with the automatic declassification provisions of the Order. All agencies with original classification authority shall cooperate with NARA in carrying out an automatic declassification program involving accessioned Federal records, presidential papers and records, and donated historical materials under the control of the Archivist of the United States. The Archivist will not declassify information created by another agency without the prior consent of that agency.

(b) *Presidential records.* The Archivist of the United States shall establish procedures for the declassification of presidential or White House materials accessioned into the National Archives of the United States or maintained in the presidential libraries.

(c) *Transferred information.* In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage or archival purposes, the receiving agency shall be deemed to be the originating agency.

(d) *Unofficially transferred information.* In the case of classified information that is not officially transferred as described in paragraph (c), of this section, but that originated in an agency that has ceased to exist and for which there is no successor agency, the Director of ISOO will designate an agency or agencies to act on provisions of the Order.

(e) *Processing records originated by another agency.* When an agency uncovers classified records originated by another agency that appear to meet the criteria for the application of the automatic declassification provisions of the Order, the finding agency should alert the originating agency and seek instruction regarding the handling and disposition of pertinent records.

(f) *Unscheduled records.* Classified information in records that have not been scheduled for disposal or retention by NARA is not subject to section 3.4 of the Order. Classified information in records that are scheduled as permanently valuable when that information is already more than 20 years old shall be subject to the automatic declassification provisions of section 3.4 of the Order five years from the date the records are scheduled. Classified information in records that are scheduled as permanently valuable when that information is less than 20 years old shall be subject to the automatic declassification provisions of section 3.4 of the Order when the information is 25 years old.

(g) *Foreign government information.* The declassifying agency is the agency that initially received or classified the information. When foreign government information appears to be subject to automatic declassification, the declassifying agency shall determine whether the information is subject to a treaty or international agreement that would prevent its declassification at that time. The declassifying agency shall also determine if another exemption under section 3.4(b) of the Order, such as the exemption that pertains to United States foreign relations, may apply to the information. If the declassifying agency believes such an exemption may apply, it should consult with any other concerned agencies in making its declassification determination. The declassifying agency or the Department of State, as appropriate, should consult with the foreign government prior to declassification.

(h) *Assistance to the Archivist of the United States.* Agencies shall consult with NARA before establishing automatic declassification programs. Agencies shall cooperate with NARA in developing schedules for the declassification of records in the National Archives of the United States and the presidential libraries to ensure that declassification is accomplished in a timely manner. NARA will provide information about the records proposed for automatic declassification. Agencies shall consult with NARA before reviewing records in their holdings to ensure that appropriate procedures are established for maintaining the integrity of the records and that NARA receives accurate information about agency declassification actions when records are transferred to NARA. NARA will provide guidance to the agencies about

the requirements for notification of declassification actions on transferred records, box labeling, and identifying exempt information in the records.

(i) *Use of approved declassification guides.* Approved declassification guides may be used as a tool to assist in the exemption from automatic declassification of specific information as provided in section 3.4(d) of the Order. These guides must include additional pertinent detail relating to the exemptions described in section 3.4(b) of the Order, and follow the format required of declassification guides for systematic review as described in 2001.53 of this part. In order for such guides to be used in place of the identification of specific information within individual documents, the information to be exempted must be narrowly defined, with sufficient specificity to allow the user to identify the information with precision. Exemptions for general categories of information will not be acceptable. The actual items to be exempted are specific documents. All such declassification guides used in conjunction with section 3.4(d) of the Order must be submitted to the Director of ISOO, serving as Executive Secretary of the Interagency Security Classification Appeals Panel, for approval by the Panel.

(j) *Automatic declassification date.* No later than April 17, 2000, information over 25 years old in unreviewed permanently valuable records in non-exempt file series will be automatically declassified.

(k) *Redaction standard.* Agencies are encouraged but are not required to redact documents that contain information that is exempt from automatic declassification under section 3.4 of the Order, especially if the information that must remain classified comprises a relatively small portion of the document.

(l) *Restricted Data and Formerly Restricted Data.* (1) Restricted Data (RD) and Formerly Restricted Data (FRD) are exempt from the automatic declassification requirements in section 3.4 of the Order because they are classified under the Atomic Energy Act of 1954, as amended. Restricted Data concerns:

(i) The design, manufacture, or utilization of atomic weapons;

(ii) The production of special nuclear material, e.g., enriched uranium or plutonium; or

(iii) The use of special nuclear material in the production of energy.

(2) Formerly Restricted Data is information that is still classified but which has been removed from the Restricted Data category because it is related primarily to the military utilization of atomic weapons.

(3) Any document marked as containing Restricted Data or Formerly Restricted Data shall remain classified indefinitely or shall be referred to the Department of Energy or the Department of Defense for a classification review.

§2001.52 *Systematic declassification review [3.5]*

(a) *Listing of declassification authorities.* Agencies shall maintain a current listing of officials delegated declassification authority by name, position, or other identifier. If possible, this listing shall be unclassified.

(b) *Responsibilities.* Agencies shall establish systematic review programs for those records containing information that is exempt from automatic declassification. Agencies may also conduct

systematic review of information contained in permanently valuable records that is less than 25 years old.

§2001.53 *Declassification guides [3.5(b)]*

(a) *Preparation of declassification guides.* Declassification guides shall be prepared to facilitate the declassification of information contained in records determined to be of permanent historical value. When it is sufficiently detailed and understandable, and identified for both purposes, a classification guide may also be used as a declassification guide.

(b) *General content of declassification guides.* Declassification guides shall, at a minimum:

(1) Identify the subject matter of the declassification guide;

(2) Identify the original declassification authority by name or personal identifier, and position;

(3) Provide the date of issuance or last review;

(4) State precisely the categories or elements of information:

(i) To be declassified;

(ii) To be downgraded; or

(iii) Not to be declassified.

(5) Identify any related files series that have been exempted from automatic declassification pursuant to section 3.4(c) of the Order;

(6) To the extent a guide is used in conjunction with the automatic declassification provisions in section 3.4 of the Order, state precisely the elements of information to be exempted from declassification to include:

(i) The appropriate exemption category listed in section 3.4(b) of the Order, and, when citing the exemption category listed in section 3.4(b)(9) of the Order, specify the applicable statute, treaty or international agreement; and

(ii) A date or event for declassification.

(c) *External review.* Agencies shall submit declassification guides for review to the Director of ISOO. To the extent such guides are used in conjunction with the automatic declassification provisions in section 3.4 of the Order, the Director shall submit them for approval by the Interagency Security Classification Appeals Panel.

(d) *Internal review and update.* Agency declassification guides shall be reviewed and updated as circumstances require, but at least once every five years. Each agency shall maintain a list of its declassification guides in use.

§2001.54 *Mandatory review for declassification [3.6, 3.7]*

(a) *U.S. originated information.*

(1) *Receipt of requests.* Each agency shall publish in the *Federal Register* the identity of the person(s) or office(s) to which mandatory declassification review requests should be addressed.

(2) *Processing.*

(i) *Requests for classified records in the custody of the originating agency.* A valid mandatory declassification review request need not identify the requested information by date or title of the responsive records, but must be of sufficient specificity to allow agency personnel to locate the records containing the information sought with a reasonable amount of effort. In responding to mandatory declassification review requests, agencies shall either make a prompt declassification determination and notify the requester accordingly, or inform the requester of the additional time needed to process the request. Agencies shall ordinarily make a final determination within 180 days from the date of receipt. When information cannot be declassified in its entirety, agencies will make reasonable efforts to release, consistent with other applicable law, those declassified portions of the requested information that constitute a coherent segment. Upon denial of an initial request, the agency shall also notify the requester of the right of an administrative appeal, which must be filed within 60 days of receipt of the denial.

(ii) *Requests for classified records in the custody of an agency other than the originating agency.* When an agency receives a mandatory declassification review request for records in its possession that were originated by another agency, it shall refer the request and the pertinent records to the originating agency. However, if the originating agency has previously agreed that the custodial agency may review its records, the custodial agency shall review the requested records in accordance with declassification guides or guidelines provided by the originating agency. Upon receipt of a request from the referring agency, the originating agency shall process the request in accordance with this section. The originating agency shall communicate its declassification determination to the referring agency.

(iii) *Appeals of denials of mandatory declassification review requests.* The agency appellate authority shall normally make a determination within 60 working days following the receipt of an appeal. If additional time is required to make a determination, the agency appellate authority shall notify the requester of the additional time needed and provide the requester with the reason for the extension. The agency appellate authority shall notify the requester in writing of the final determination and of the reasons for any denial.

(iv) *Appeals to the Interagency Security Classification Appeals Panel.* In accordance with section 5.4 of the Order, the Interagency Security Classification Appeals Panel shall publish in the *Federal Register* no later than February 12, 1996, the rules and procedures for bringing mandatory declassification appeals before it.

(b) *Foreign government information.* Except as provided in this paragraph, agency heads shall process mandatory declassification review requests for classified records containing foreign government information in accordance with this section. The declassifying agency is the agency that initially received or classified the information. When foreign government information is being considered for declassification, the declassifying agency shall determine whether the information is subject to a treaty or international agreement that would prevent its declassification at that time. The declassifying agency shall also determine if another

exemption under section 1.6(d) of the Order (other than section 1.6(b)(5)), such as the exemption that pertains to United States foreign relations, may apply to the information. If the declassifying agency believes such an exemption may apply, it should consult with any other concerned agencies in making its declassification determination. The declassifying agency or the Department of State, as appropriate, should consult with the foreign government prior to declassification.

(c) *Cryptologic and intelligence information.* Mandatory declassification review requests for cryptologic information and information concerning intelligence activities (including special activities) or intelligence sources or methods shall be processed solely in accordance with special procedures issued by the Secretary of Defense and the Director of Central Intelligence, respectively.

(d) *Fees.* In responding to mandatory declassification review requests for classified records, agency heads may charge fees in accordance with section 9701 of title 31, United States Code. The schedules of fees published in the *Federal Register* by agencies in implementation of Executive Order 12356 shall remain in effect until revised.

(e) *Assistance to the Department of State.* Heads of agencies should assist the Department of State in its preparation of the *Foreign Relations of the United States* (FRUS) series by facilitating access to appropriate classified materials in their custody and by expediting declassification review of documents proposed for inclusion in the FRUS.

(f) *Requests filed under mandatory declassification review and the Freedom of Information Act.* When a requester submits a request both under mandatory review and the Freedom of Information Act (FOIA), the agency shall require the requester to elect one process or the other. If the requester fails to elect one or the other, the request will be treated as a FOIA request unless the requested materials are subject only to mandatory review.

(g) *FOIA and Privacy Act requests.* Agency heads shall process requests for declassification that are submitted under the provisions of the FOIA, as amended, or the Privacy Act of 1974, in accordance with the provisions of those Acts.

(h) *Redaction standard.* Agencies shall redact documents that are the subject of an access demand unless the overall meaning or informational value of the document is clearly distorted by redaction.

Subpart F - Reporting

§2001.60 *Statistical reporting [5.3]*

Each agency that creates or handles classified information shall report annually to the Director of ISOO statistics related to its security classification program. The Director shall solicit recommendations from the member agencies of the Security Policy Forum regarding the reporting requirements. The Director will instruct agencies what data elements are required, and how and when they are to be reported.

§2001.61 *Accounting for costs [5.6(c)(8)]*

(a) Information on the costs associated with the implementation of the Order will be collected from the agencies by the Office of Management and Budget (OMB). OMB will provide data to ISOO on the cost estimates for classification-related activities. ISOO will include these cost estimates in its annual report to the President. The agency senior official should work closely with the agency comptroller to ensure that the best estimates are collected.

(b) The Secretary of Defense, acting as the executive agent for the National Industrial Security Program under Executive Order 12829, and consistent with agreements entered into under section 202 of E.O. 12829, will collect cost estimates for classification-related activities of contractors, licensees, certificate holders, and grantees, and report them to ISOO annually. ISOO will include these cost estimates in its annual report to the President.

§2001.62 *Effective date [6.2]*

Part 2001 shall become effective October 14, 1995.

Alice M. Rivlin

Director
Office of Management and Budget